Computing Rational Points in Convex Semialgebraic Sets and Sum of Squares Decompositions

Mohab Safey El Din, Lihong Zhi

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Computing rational points in convex semi-algebraic sets and SOS decompositions

Mohab Safey El Din — Lihong Zhi

N° 7045

Septembre 2009

Rapport de recherche

ISSN 0249-6399 ISRN INRIA/RR--7045--FR+ENG

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

INRIA

centre de recherche PARIS - ROCQUENCOURT

Computing rational points in convex semi-algebraic sets and SOS decompositions

Mohab Safey El Din*, Lihong Zhi†

Thème : Algorithmique, calcul certifié et cryptographie
Équipe-Projet SALSA

Rapport de recherche n° 7045 — Septembre 2009 — 18 pages

Abstract: Let $\mathcal{P} = \{h_1, \ldots, h_s\} \subset \mathbb{Z}[Y_1, \ldots, Y_k]$, $D \geq \deg(h_i)$ for $1 \leq i \leq s$, σ bounding the bit length of the coefficients of the h_i's, and Φ be a quantifier-free $\mathcal{P}$-formula defining a convex semi-algebraic set. We design an algorithm returning a rational point in $\mathcal{S}$ if and only if $\mathcal{S} \cap \mathbb{Q} \neq \emptyset$. It requires $\sigma^{\mathrm{O}(1)} D^{\mathrm{O}(k^3)}$ bit operations. If a rational point is outputted its coordinates have bit length dominated by $\sigma D^{\mathrm{O}(k^3)}$. Using this result, we obtain a procedure deciding if a polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$ is a sum of squares of polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$. Denote by d the degree of f, τ the maximum bit length of the coefficients in f, $D = \binom{n+d}{n}$ and $k \leq D(D+1) - \binom{n+2d}{n}$. This procedure requires $\tau^{\mathrm{O}(1)} D^{\mathrm{O}(k^3)}$ bit operations and the coefficients of the outputted polynomials have bit length dominated by $\tau D^{\mathrm{O}(k^3)}$.

Key-words: rational sum of squares, semidefinite programming, convex semi-algebraic sets, complexity.

* UPMC, Paris 6, LIP6
† KLMM, Academy of Mathematics and System Sciences, China

Centre de recherche INRIA Paris – Rocquencourt
Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex
Téléphone : +33 1 39 63 55 11 — Télécopie : +33 1 39 63 53 30

Calcul de points rationnels dans des semi-algébriques convexes et décomposition en sommes de carrés

Résumé : Soit $\mathcal{P} = \{h_1, \ldots, h_s\} \subset \mathbb{Z}[Y_1, \ldots, Y_k]$, $D \geq \deg(h_i)$ pour $1 \leq i \leq s$, σ une borne sur la longueur binaire des coefficients des h_i, et Φ une $\mathcal{P}$-formule sans quantificateurs définissant un ensemble semi-algébrique convexe. Nous décrivons un algorithme qui retourne un point à coordonnées rationnelles dans $\mathcal{S}$ si et seulement si $\mathcal{S} \cap \mathbb{Q} \neq \emptyset$. Cet algorithme est de complexité binaire $\sigma^{\mathrm{O}(1)} D^{\mathrm{O}(k^3)}$. Si un point rationnel est renvoyé, ses coordonnées sont de longueur binaires dominées par $\sigma D^{\mathrm{O}(k^3)}$. On déduit de ce résultat une procédure qui décide si un polynôme $f \in \mathbb{Z}[X_1, \ldots, X_n]$ est une somme de carrés de polynômes dans $\mathbb{Q}[X_1, \ldots, X_n]$. Soit d le degré de f, τ le maximum des longueurs binaires des coefficients de f, $D = \binom{n+d}{n}$ et $k \leq D(D+1) - \binom{n+2d}{n}$. Cette procédure est de complexité binaire $\tau^{\mathrm{O}(1)} D^{\mathrm{O}(k^3)}$ et les coefficients des polynômes obtenus en sortie ont une longueur binaire dominée par $\tau D^{\mathrm{O}(k^3)}$.

Mots-clés : sommes de carrés à coefficients rationnels, programmation semi-définie positive, ensembles semi-algebraiques convexes, complexité.

1 Introduction

Motivation and problem statement. Suppose $f \in \mathbb{R}[x_1, \ldots, x_n]$, then f is a sum of squares (SOS) in $\mathbb{R}[x_1, \ldots, x_n]$ if and only if it can be written in the form

$$f = \mathrm{v}^T \cdot M \cdot \mathrm{v}, \tag{1}$$

in which v is a column vector of monomials and M is a real positive semidefinite matrix (Powers and Wörmann, 1998, Theorem 1) (see also Choi et al. (1995)). M is also called a *Gram matrix* for f. If M has rational entries, then f is a sum of squares in $\mathbb{Q}[x_1, \ldots, x_n]$.

PROBLEM 1.1 *(Sturmfels). If $f \in \mathbb{Q}[x_1, \ldots, x_n]$ is a sum of squares in $\mathbb{R}[x_1, \ldots, x_n]$, then is f also a sum of squares in $\mathbb{Q}[x_1, \ldots, x_n]$?*

It has been pointed out that if there is an invertible Gram matrix for f, then there is a Gram matrix for f with rational entries (Hillar, 2009, Theorem 1.2). Furthermore, if $f \in \mathbb{Q}[x_1, \ldots, x_n]$ is a sum of m squares in $K[x_1, \ldots, x_n]$, where K is a totally real number field with Galois closure L, then f is also a sum of $4m \cdot 2^{[L:\mathbb{Q}]+1}\binom{[L:\mathbb{Q}]+1}{2}$ squares in $\mathbb{Q}[x_1, \ldots, x_n]$ (Hillar, 2009, Theorem 1.4). It is interesting to see that the number of squares can be reduced to m (see Kaltofen (2009)).

Although no example is known of a rational polynomial having only irrational sum of squares, a complete answer to Question 1.1 is not known. This is the main motivation for us to design an algorithm to check whether a rational polynomial having a rational sum of squares decomposition and give the rational SOS representation if it does exist. By reducing this problem to semi-definite programming, this can be done by designing an algorithm checking if a convex semi-algebraic set contains rational points (see Powers and Wörmann (1998)).

Main result. We propose an algorithm which decides if a *convex* semi-algebraic set $\mathcal{S} \subset \mathbb{R}^k$ contains rational points (i.e. points with coordinates in $\mathbb{Q}^k$). In the case where $\mathcal{S} \cap \mathbb{Q}^k$ is non-empty, a rational point in $\mathcal{S}$ is computed.

The semi-algebraic set $\mathcal{S}$ is given as the solution set of a polynomial system of non-strict inequalities with integer coefficients. Arithmetic operations, sign evaluations and comparisons of two integers/rationals can be done in polynomial time of the maximum bit length of the considered integers/rationals.

We bound the number of bit operations that the algorithm performs with respect to the number of polynomials, their degrees and the maximum bit length of their input coefficients; we also give upper bounds on the bit length of the coordinates of the outputted rational point if this situation occurs. More precisely, the main result is as follows.

Theorem 1.1 *Consider a set of polynomials $\mathcal{P} = \{h_1, \ldots, h_s\} \subset \mathbb{Z}[Y_1, \ldots, Y_k]$, and a quantifier-free $\mathcal{P}$-formula $\Phi(Y_1, \ldots, Y_k)$ and let D be an integer such that $\deg(h_i) \leq D$ for $1 \leq i \leq s$ and σ the maximum bit length of the coefficients of the h_i's. Let $\mathcal{S} \subset \mathbb{R}^k$ be the convex semi-algebraic set defined by Φ. There exists an algorithm which decides if $\mathcal{S} \cap \mathbb{Q}^k$ is non-empty within $\sigma^{\mathrm{O}(1)}(sD)^{\mathrm{O}(k^3)}$ bit operations. In case of non-emptiness, it returns an element of $\mathcal{S} \cap \mathbb{Q}^k$ whose coordinates have bit length dominated by $\sigma D^{\mathrm{O}(k^3)}$.*

We use a procedure due to Basu et al. (1996) performing quantifier elimination over the reals in order to deduce from Theorem 1.1 the following result.

Corollary 1.2 *Let $\mathcal{S} \subset \mathbb{R}^k$ be a convex set defined by*

$$\mathcal{S} = \{Y \in \mathbb{R}^k : (Q_1 X^{[1]} \in \mathbb{R}^{n_1}) \cdots (Q_\omega X^{[\omega]} \in \mathbb{R}^{n_\omega})\ P(Y, X^{[1]}, \ldots, X^{[\omega]})\}$$

with quantifiers $Q_i \in \{\exists, \forall\}$, where $X^{[i]}$ is a set of n_i variables, P is a Boolean function of s atomic predicates

$$g(Y, X^{[1]}, \ldots, X^{[\omega]})\, \Delta_i\, 0$$

where $\Delta_i \in \{>, <, =\}$ (for $i = 1, \ldots, s$) and the g_i's are polynomials of degree D with integer coefficients of binary size at most σ. There exists an algorithm which decides if $\mathcal{S} \cap \mathbb{Q}^k$ is non-empty within $\sigma^{\mathrm{O}(1)}(sD)^{\mathrm{O}(k^3 \Pi_{i=1}^{\omega} n_i)}$ bit operations. In case of non-emptiness, it returns an element of $\mathcal{S} \cap \mathbb{Q}^k$ whose coordinates have bit length dominated by $\sigma D^{\mathrm{O}(k^3 \Pi_{i=1}^{\omega} n_i)}$.

The proof of the above results is based on quantitative and algorithmic results for computing sampling points in semi-algebraic sets and quantifier elimination over the reals.

It is well-known that deciding if a given polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$ of degree d whose coefficients have bit length dominated by τ is a sum of squares of polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ can be reduced to a linear matrix inequality which defines a convex semi-algebraic set (see e.g. Powers and Wörmann (1998)). Applying Theorem 1.1, we show that there exists an algorithm deciding if such an SOS decomposition exists over the rationals and that the coefficients of the polynomials in the decomposition have bit length dominated by $\tau D^{\mathrm{O}(k^3)}$ with $D = \binom{n+d}{n}$ and $k \leq D(D+1) - \binom{n+2d}{n}$. Moreover, such a decomposition can be found within $\tau^{\mathrm{O}(1)} D^{\mathrm{O}(k^3)}$ bit operations.

Prior works. Khachiyan and Porkolab extended the well-known result of Lenstra (1983) on the polynomial-time solvability of linear integer programming in fixed dimension to semidefinite integer programming. The following proposition is given in Khachiyan and Porkolab (1997, 2000).

Proposition 1.3 *Let $\mathcal{S} \subset \mathbb{R}^k$ be a convex set defined as in Corollary 1.2. There exists an algorithm for solving the problem* $\min\{Y_k | Y = (Y_1, \ldots, Y_k) \in \mathcal{S} \bigcap \mathbb{Z}^k\}$ *in time $\ell^{\mathrm{O}(1)}(sD)^{\mathrm{O}(k^4)\Pi_{i=1}^{\omega}\mathrm{O}(n_i)}$. In case of non-empty, then the minimization problem has an optimal solution whose bit length is dominated by $\ell D^{\mathrm{O}(k^4)\Pi_{i=1}^{\omega}\mathrm{O}(n_i)}$.*

Their algorithm was further improved by Heinz for the case of convex minimization where the feasible region is described by quasiconvex polynomials Heinz (2005).

Although we can apply Proposition 1.3 directly to certify that a given polynomial with integer coefficients to be non-negative for all real values of the variables by computing a sum of squares in $\mathbb{Z}[x_1, \ldots, x_n]$, the nonnegativity of a polynomial can be certified if it can be written as a sum of squares of polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$. Some hybrid symbolic-numeric algorithms have been given in Peyrl and Parrilo (2007, 2008); Kaltofen et al. (2008, 2009) which turn a numerical sum of squares representation of a positive polynomial into an exact rational identity. However, it is well known that there are plenty of polynomials which are nonnegative but can not be written as sums of squares of polynomials, for example, the famous Motzkin polynomial. This also impel us to study Khachiyan and Porkolab's approach. It turns out that by focusing on rational numbers instead of integers, we can design an exact algorithm which decide whether a given polynomial can be written as an SOS over the rationals and give the rational SOS decomposition if it exists.

Structure of the paper. Section 2 is devoted to recall the quantitative and algorithmic results on computing sampling points in semi-algebraic sets and quantifier elimination over the reals. Most of these results are proved in Basu et al. (1996). Section 3 is devoted to prove the correctness of the algorithm on which Theorem 1.1 and Corollary 1.2 rely. The complexity analysis is done in Section 4. In Section 5, we apply Theorem 1.1 to prove the announced bounds on the bit length of the rational coefficients of the decomposition into sums of squares of a given polynomial with integer coefficients.

Acknwledgments. This work is supported by the EXACTA grant of National Science Foundation of China (NSFC) and the French National Research Agency (ANR). The authors thank INRIA, KLMM and the Academy of Mathematics and System Sciences for their support.

2 Preliminaries

The algorithm on which Theorem 1.1 relies and its complexity analysis are based on algorithmic and quantitative results on computing sampling points in semi-algebraic sets and quantifier elimination over the reals.

2.1 Computing points in semi-algebraic sets

Consider a set of polynomials $\mathcal{P} = \{h_1, \dots, h_J\} \subset \mathbb{Z}[Y_1, \dots, Y_k]$, and a quantifier-free $\mathcal{P}$-formula $\Phi(Y_1, \dots, Y_k)$ (i.e. a quantifier-free formula whose atoms is one of $h = 0$, $h \neq 0$, $h > 0$, $h < 0$ for $h \in \mathcal{P}$). Let D be an integer such that $\deg(h_i) \leq D$ for $1 \leq i \leq J$ and ℓ the maximum bit length of the coefficients of the h_i's. We denote by $\mathcal{S} \subset \mathbb{R}^k$ the semi-algebraic set defined by $\Phi(Y_1, \dots, Y_k)$.

A function RealizableSignConditions computing a set of algebraic points having a non-empty intersection with each connected component of semi-algebraic sets defined by sign conditions satisfied by $\mathcal{P}$ is given in (Basu et al., 1996, Section 3) (see also (Basu et al., 2006, Chapter 5)). From this, a function SamplingPoints computing a set of algebraic points having a non-empty intersection with each connected component of $\mathcal{S}$ is obtained. These algebraic points are encoded by

- a rational parametrization

$$G = 0, Y_1 = \frac{G_1}{G_0}, \dots, Y_k = \frac{G_k}{G_0}$$

where $G, G_0, \dots, G_k$ are polynomials in $\mathbb{Z}[T]$ such that $\deg(\gcd(G, G_0)) = 0$ and

for $1 \le i \le k$, $-1 \le \deg(G_i) \le \deg(G) - 1$ and $0 \le \deg(G_0) \le \deg(G) - 1$;

the rational parametrization is given by the list $\mathcal{G} = (G, G_0, G_1, \dots, G_k)$; the degree of $\mathcal{G}$ is called *degree of the rational parametrization* and $Z(\mathcal{G}) \subset \mathbb{C}^k$ denotes the set of complex points encoded by $\mathcal{G}$;

- and a list $\mathcal{T}$ of the Thom-encodings of the real roots ϑ of G such that $\Phi\left(\frac{G_1(\vartheta)}{G_0(\vartheta)}, \dots, \frac{G_k(\vartheta)}{G_0(\vartheta)}\right)$ is true.

The bit complexity of SamplingPoints is $\ell J^{k+1} D^{\mathrm{O}(k)}$ and the output is such that $\deg(G) = \mathrm{O}(D)^k$ and the bit length of the coefficients of $G, G_0, G_1, \dots, G_k$ is dominated by $\ell D^{\mathrm{O}(k)}$.

Factorizing over $\mathbb{Q}$ a univariate polynomial $h \in \mathbb{Q}[T]$ of degree δ with rational coefficients of maximum bit length ℓ can be done in $\ell^{\mathrm{O}(1)}\delta^{\mathrm{O}(1)}$ bit-operations (see Lenstra et al. (1982); van Hoeij and Novocin (2007); Schönhage (1984)). Given a root ϑ of h, the minimal polynomial of ϑ has coefficients of bit length dominated by $\ell + \mathrm{O}(\delta)$ (see Mignotte (1982)).

Consider now a root ϑ of G and its minimal polynomial g. Since G and G_0 are co-prime, one can compute $G_0^{-1} \mod g$ to obtain a rational parametrization $(g, g_0, \dots, g_k)$ with integer coefficients of bit length dominated by $\ell D^{\mathrm{O}(k)}$ and

for $1 \le i \le k$, $-1 \le \deg(g_i) \le \deg(g) - 1$ and $0 \le \deg(g_0) \le \deg(g) - 1$

within a bit-complexity $\ell^{\mathrm{O}(1)} D^{\mathrm{O}(k)}$. This implies the following result.

Proposition 2.1 *There exists a function* SemiAlgebraicSolve *which takes as input the system $\Phi(Y_1, \dots, Y_k)$ and computes a rational parametrization $\mathcal{G} = (G, G_0, G_1, \dots, G_k)$ and a list $\mathcal{T}$ of Thom-encodings such that G is irreducible over $\mathbb{Q}$, and $\mathcal{T}$ contains the encodings of the real roots ϑ of G such that $\left(\frac{G_1(\vartheta)}{G_0(\vartheta)}, \dots, \frac{G_k(\vartheta)}{G_0(\vartheta)}\right) \in \mathcal{S}$. The bit length of the coefficients of $G, G_0, G_1, \dots, G_k$ is dominated by $\ell D^{\mathrm{O}(k)}$ and $\deg(G) = \mathrm{O}(D)^k$. Moreover,* SemiAlgebraicSolve *requires $\ell^{\mathrm{O}(1)} J^{k+1} D^{\mathrm{O}(k)}$ bit operations.*

Remark 2.2 *Since G and G_0 are co-prime, one can compute ${G_0}^{-1} \mod G$ in polynomial time, and the binary length of its rational coefficients can be bounded via subresultants, we can assume, without loss of generality, that the rational parametrization has a constant denominator:*

$$Y = \frac{1}{q}(G_1(\vartheta), G_2(\vartheta), \dots, G_k(\vartheta)) \in \mathcal{S}, \ G(\vartheta) = 0, \tag{2}$$

where the bit length of q and the coefficients of $G, G_1, \dots, G_k$ are dominated by $\ell D^{\mathrm{O}(k)}$.

The above discussion leads also to the following result.

Proposition 2.3 *Let $\mathcal{G}, \mathcal{T}$ be the output of* SemiAlgebraicSolve(Φ)*, δ be the degree of G, and ℓ be the maximum bit length of the coefficients of the polynomials in $\mathcal{G} \cup \mathcal{P}$. There exists a function* RationalZeroDimSolve *which takes* *as input $\mathcal{G}$ and Φ and returns a rational point $y \in Z(\mathcal{G})$ if and only if $y \in \mathcal{S} \cap Z(\mathcal{G}) \cap \mathbb{Q}^k$, else it returns an empty list. The coordinates of these rational points have bit length dominated by $\ell\delta^{\mathrm{O}(1)}$ and computations are performed within $\mathrm{O}(k)\mathrm{O}(J)\ell^{\mathrm{O}(1)}\delta^{\mathrm{O}(1)}\binom{n+D}{n}^{\mathrm{O}(1)}$ bit operations.*

Remark 2.4 *According to Proposition 2.1, the function* SemiAlgebraicSolve *computes a rational parametrization $\mathcal{G} = (G, G_0, G_1, \ldots, G_k)$ such that G is irreducible over $\mathbb{Q}$. Therefore a rational point $y \in Z(\mathcal{G})$ if and only if $\deg(G) = 1$. In order to check whether $y \in \mathcal{S}$, we only need to evaluate the formula Φ at y.*

The following result is a restatement of (Basu et al., 1996, Theorem 4.1.2) and allows us to bound the bit length of rational points in non-empty semi-algebraic sets defined by strict polynomial inequalities.

Proposition 2.5 *Let $\mathcal{S}' \subset \mathbb{R}^k$ be a semi-algebraic set defined by a quantifier-free $\mathcal{P}$-formula whose atoms are strict inequalities. Then $\mathcal{S}'$ contains a rational point whose coordinates have bit length dominated by $\ell D^{\mathrm{O}(k)}$.*

The proof of the above result (see (Basu et al., 1996, Proof of Theorem 4.1.2 pp. 1032)) is based on the routine RealizableSignConditions and the isolation of real roots of univariate polynomials with rational coefficients (see e.g. (Basu et al., 2006, Chapter 10)). We denote by RationalOpenSemiAlgebraicSolve a function taking as input the $\mathcal{P}$-formula Φ and which returns a rational point in $\mathcal{S}$ if and only if there exists a non-empty semi-algebraic set $\mathcal{S}'$ defined by a quantifier-free $\mathcal{P}$-formula whose atoms are strict inequalities such that $\mathcal{S}' \subset \mathcal{S}$. The result below is not stated in Basu et al. (1996) but is an immediate consequence of this proof.

Corollary 2.6 *Suppose that there exists a quantifier-free $\mathcal{P}$-formula whose atoms are strict inequalities defining a non-empty semi-algebraic set $\mathcal{S}' \subset \mathcal{S}$. There exists an algorithm computing a rational point in $\mathcal{S}$ if and only if $\mathcal{S} \neq \emptyset$. It requires $\ell^{\mathrm{O}(1)}J^{k+1}D^{\mathrm{O}(k)}$ bit operations and if a rational point is outputted, its coordinates have bit length dominated by $\ell D^{\mathrm{O}(k)}$.*

2.2 Quantifier elimination over the reals

We consider now a first-order formula F over the reals

$$(Q_1 X^{[1]} \in \mathbb{R}^{n_1}) \cdots (Q_\omega X^{[\omega]} \in \mathbb{R}^{n_\omega})\ P(Y, X^{[1]}, \ldots, X^{[\omega]})$$

where

- $Y = (Y_1, \ldots, Y_k)$ is the vector of free variables;
- each Q_i $(i = 1, \ldots, \omega)$ is one of the quantifiers $\exists$ or $\forall$;
- $P(Y, X^{[1]}, \ldots, X^{[\omega]})$ is a Boolean function of s atomic predicates

$$g(Y, X^{[1]}, \ldots, X^{[\omega]})\, \Delta_i\, 0$$

  where $\Delta_i \in \{>, <, =\}$ (for $i = 1, \ldots, s$) and the g_i's are polynomials of degree D with integer coefficients of binary size at most ℓ.

The following result on quantifier elimination is a restatement of (Basu et al., 1996, Theorem 1.3.1).

Theorem 2.7 *There exists a quantified-free formula* Ψ

$$\bigvee_{i=1}^{I}\bigwedge_{j=1}^{J_i}(h_{ij}\,\Delta_{ij}\,0)$$

(where $h_{ij}\in\mathbb{Z}[Y_1,\ldots,Y_k]$ *and* $\Delta_{ij}\in\{=,>\}$*) which is equivalent to* F *and such that*

- $I\le s^{(k+1)\Pi_{i=1}^{\omega}(n_i+1)}D^{(k+1)\Pi_{i=1}^{\omega}\mathrm{O}(n_i)}$,
- $J_i\le s^{\Pi_{i=1}^{\omega}(n_i+1)}D^{\Pi_{i=1}^{\omega}\mathrm{O}(n_i)}$,
- $\deg(h_{ij})\le D^{\Pi_{i=1}^{\omega}\mathrm{O}(n_i)}$,
- *the bit length of the coefficients of the polynomials* h_{ij} *is dominated by* $\ell D^{(k+1)\Pi_{i=1}^{\omega}\mathrm{O}(n_i)}$.

The above transformation requires $\ell s^{(k+1)\Pi_{i=1}^{\omega}(n_i+1)}D^{(k+1)\Pi_{i=1}^{\omega}\mathrm{O}(n_i)}$ *bit operations.*

In the sequel, we denote by QuantifierElimination a function that takes F as input and returns a list $[\Psi_1,\ldots,\Psi_I]$ where the $\Psi_i's$ are the conjunctions

$$\bigwedge_{j=1}^{J_i}(h_{ij}\,\Delta_{ij}\,0).$$

3 Algorithm and correctness

3.1 Description of the algorithm

We use the following functions:

- Substitute which takes as input a variable $Y_r\in\{Y_1,\ldots,Y_k\}$, a polynomial $h\in\mathbb{Q}[Y_1,\ldots,Y_k]$ and a Boolean formula F and which returns a formula $\tilde{F}$ obtained by substituting Y_r by h in F.
- RemoveDenominators which takes as input a formula F and returns a formula $\tilde{F}$ obtained by multiplying the polynomials in F by the absolute value of the lcm of the denominators of their coefficients.

Consider now a rational parametrization $\mathcal{G}=(G,G_0,G_1,\ldots,G_k,G_{k+1})\subset\mathbb{Z}[T]^{k+3}$ with $\delta=\deg(G)$. For $0\le i\le\delta-1$, denote by $\mathbf{a}_i\in\mathbb{Z}^k$ the vector of integers whose j-th coordinate is the coefficient of T^i in G_j. Similarly, for $0\le i\le\delta-1$, $\mathbf{b}_i$ denotes the coefficient of T^i in G_{k+1}. We use in the sequel a function GenerateVectors that takes as input a rational parametrization $\mathcal{G}$. This function returns the set list of couples $(\mathbf{a}_i,\mathbf{b}_i)$ for $0\le i\le\delta-1$.

As in the previous section, consider now a set of polynomials $\mathcal{P}=\{h_1,\ldots,h_s\}\subset\mathbb{Z}[Y_1,\ldots,Y_k]$, and a quantifier-free $\mathcal{P}$-formula $\Phi(Y_1,\ldots,Y_k)$ and let D be an integer such that $\deg(h_i)\le D$ for $1\le i\le s$ and σ the maximum bit length of the coefficients of the h_i's. We denote by $\mathcal{S} \subset \mathbb{R}^k$ the semi-algebraic set defined by $\Phi(Y_1, \ldots, Y_k)$ which is supposed to be convex.

The routine FindRationalPoints below takes as input the formula $\Phi(Y_1, \ldots, Y_k)$ defining $\mathcal{S} \subset \mathbb{R}^k$ and the list of variables $[Y_1, \ldots, Y_k]$.

FindRationalPoints$(\Phi, [Y_1, \ldots, Y_k])$.

1. Let $L = \mathsf{RationalOpenSemiAlgebraicSolve}(\mathsf{Open}(\Phi))$
2. If L is not empty then return L
3. Let $\mathcal{G}, \mathcal{T} = \mathsf{SemiAlgebraicSolve}(\Phi)$
4. If $\mathcal{T}$ is empty then return []
5. Let $L = \mathsf{RationalZeroDimSolve}(\mathcal{G}, \Phi)$
6. If L is not empty or $k = 1$ then return L
7. Else
   (a) Let $A_1, \ldots, A_k, B$ be free variables and Θ be the formula
   $$\forall Y \in \mathbb{R}^k \quad A_1^2 + \cdots + A_k^2 > 0 \wedge (\neg\Phi \vee A_1Y_1 + \cdots + A_kY_k = B)$$
   (b) Let $[\Psi_1, \ldots, \Psi_I] = \mathsf{QuantifierElimination}(\Theta)$ and $i = 1$
   (c) While $i \leq I$ do
      i. $\mathcal{G}, \mathcal{T} = \mathsf{SemiAlgebraicSolve}(\Psi_i)$ and $(G, G_0, G_1, \ldots, G_k, G_{k+1}) = \mathcal{G}$
      ii. If $\mathcal{T}$ is empty $i = i + 1$ else break.
   (d) Let $C = \mathsf{GenerateVectors}(G, G_0, G_1, \ldots, G_k, G_{k+1})$
   (e) Let $a = (a_1, \ldots, a_k) \neq (0, \ldots, 0)$ and $b \in \mathbb{Z}$ such that $(a, b) \in C$
   (f) Let $r = \max(i, 1 \leq i \leq k \text{ and } a_i \neq 0)$
   (g) Let $h = b - \frac{\sum_{j=1}^{r-1} a_i Y_i}{a_r}$
   (h) Let $\Phi' = \mathsf{RemoveDenominators}(\mathsf{Substitute}(Y_r, h, \Phi))$
   (i) Let $L = \mathsf{FindRationalPoints}(\Phi', [Y_1, \ldots, Y_{r-1}, Y_{r+1}, \ldots, Y_k])$
   (j) If L is not empty,
      i. Let $(q_1, \ldots, q_{r-1}, q_{r+1}, \ldots, q_k)$ be its element;
      ii. Let $q_r = \mathsf{Evaluate}(\{Y_i = q_i,\ 1 \leq i \leq k,\ j \neq r\}, h)$
      iii. if $\Phi(q_1, \ldots, q_{r-1}, q_r, q_{r+1}, \ldots, q_k)$ is true, return $[(q_1, \ldots, q_{r-1}, q_r, q_{r+1}, \ldots, q_k)]$ else return [].
   (k) Else return [].

Proposition 3.1 *The algorithm* FindRationalPoints *returns a list containing a rational point if and only if* $\mathcal{S} \cap \mathbb{Q}^k$ *is non-empty, else it returns an empty list.*

The next paragraph is devoted to prove this proposition.

Remark 3.2 *Let $\mathcal{S} \subset \mathbb{R}^k$ be a convex set defined by*

$$\mathcal{S} = \{Y \in \mathbb{R}^k : \mathbb{R}^k(Q_1 X^{[1]} \in \mathbb{R}^{n_1}) \cdots (Q_\omega X^{[\omega]} \in \mathbb{R}^{n_\omega})\ P(Y, X^{[1]}, \ldots, X^{[\omega]})\}$$

with quantifiers $Q_i \in \{\exists, \forall\}$, where $X^{[i]}$ is a set of n_i variables, P is a Boolean function of s atomic predicates

$$g(Y, X^{[1]}, \ldots, X^{[\omega]})\, \Delta_i\, 0$$

where $\Delta_i \in \{>, <, =\}$ (for $i = 1, \ldots, s$).

Denote by Θ the quantified formula defining $\mathcal{S}$ and by $[\Psi_1, \ldots, \Psi_I]$ the output of QuantifierElimination(Θ)*. Running* FindRationalPoints *on the Ψ_i's allows to decide the existence of rational points in $\mathcal{S}$. This proves a part of Corollary 1.2.*

3.2 Proof of correctness

In the sequel, we denote by $\mathrm{clos}_{\mathrm{Zar}}(\mathcal{S})$ its Zariski-closure. Following (Bochnak et al., 1998, Definition 2.8.1 and Proposition 2.8.2 pp. 50), we define the *dimension* of $\mathcal{S}$ as the Krull dimension of the ideal associated to $\mathrm{clos}_{\mathrm{Zar}}(\mathcal{S})$. By convention, the dimension of the empty set is -1.

We reuse the notations introduced in the description of FindRationalPoints. The proof is done by induction on k. Before investigating the case $k = 1$, we recall some elementary facts.

Preliminaries.

We start with a lemma.

Lemma 3.3 *Let $A \subset \mathbb{R}^k$ be a semi-algebraic set defined by a quantifier-free $\mathcal{P}$-formula. If $\dim(A) = k$ there exists $y \in \mathbb{R}^k$ such that for all $h \in \mathcal{P}$ $h(y) > 0$ or $h(y) < 0$.*

Proof. Suppose that for all $y \in A$, there exists $h \in \mathcal{P}$ such that $h(y) = 0$. Then, A is contained in the union $\mathcal{H}$ of the hypersurfaces defined by $h = 0$ for $h \in \mathcal{P}$. Consequently, $\dim(A) \leq \dim(\mathcal{H}) < k$, which contradicts $\dim(A) = k$. □

The following lemma recalls an elementary property of convex semi-algebraic sets of dimension 0.

Lemma 3.4 *Let $A \subset \mathbb{R}^k$ be a convex semi-algebraic set. If $\dim(A) = 0$, then A is reduced to a single point.*

Proof. If there exist two distinct points y_1, y_2 in A, the set $B = \{ty_1 + (1 - t)y_2, t \in [0, 1]\}$ is contained in A. This implies that $\mathrm{clos}_{\mathrm{Zar}}(B) \subset \mathrm{clos}_{\mathrm{Zar}}(A)$ and consequently $\dim(B) \leq \dim(A)$. Since $\mathrm{clos}_{\mathrm{Zar}}(B)$ is the line containing y_1 and y_2, $\dim(B) = 1$ and $\dim(A) \geq 1$ which contradicts the assumption $\dim(A) = 0$. Our claim follows. □

Correctness when $k = 1$.

Lemma 3.5 *Suppose that $k = 1$. Then Steps (1-6) return a rational point in $\mathcal{S}$ if and only if $\mathcal{S} \cap \mathbb{Q}^k \neq \emptyset$ else an empty list is returned.*

Proof. If $k = 1$, the dimension of $\mathcal{S}$ is either 1, -1 or 0.

1. Suppose that $\mathcal{S}$ has dimension 1. From Lemma 3.3, there exists a non-empty semi-algebraic set $\mathcal{S}' \subset \mathcal{S}$ defined by a quantifier-free $\mathcal{P}$-formula whose atoms are strict inequalities. Thus $\mathcal{S}'$ contains a rational point. From Corollary 2.6, such a rational point in $\mathcal{S}$ is outputted at Step (1).

2. Suppose that $\mathcal{S}$ has dimension -1 (i.e. $\mathcal{S}$ is empty). From Proposition 2.1, the list of Thom-encodings outputted at Step (3) is empty and the empty list is returned at Step (4).

3. Suppose that $\mathcal{S}$ has dimension 0. From Lemma 3.4, $\mathcal{S}$ is a single point contained in $Z(\mathcal{G})$. From Proposition 2.3, this point is outputted at Step (5) if and only if it is a rational point; else the empty list is outputted.

□

The case $k > 1$.

Our induction assumption is that, given a quantifier-free $\mathcal{P}'$-formula Φ' (with $\mathcal{P}' \subset \mathbb{Z}[Y_1, \ldots, Y_{k-1}]$) defining a convex semi-algebraic set $\mathcal{S}' \subset \mathbb{R}^{k-1}$, FindRationalPoints returns a list containing a rational point if and only if $\mathcal{S}' \cap \mathbb{Q}^{k-1}$ is non-empty, else it returns an empty list.

Lemma 3.6 *Suppose that* $0 \leq \dim(\mathcal{S}) < k$. *There exists* $(a_1, \ldots, a_k) \in \mathbb{R}^k$ *and* $b \in \mathbb{R}$ *such that* $(a_1, \ldots, a_k) \neq (0, \ldots, 0)$ *and*

$$\forall (y_1, \ldots, y_k) \in \mathbb{R}^k \quad (y_1, \ldots, y_k) \in \mathcal{S} \Longrightarrow a_1 y_1 + \cdots + a_k y_k = b. \tag{3}$$

Proof. It is sufficient to prove that $\mathrm{clos}_{\mathrm{Zar}}(\mathcal{S})$ is an affine subspace over $\mathbb{R}$: in this case, there exists a real affine hyperplane H (defined by $\sum_{i=1}^{k} a_i Y_i = b$ for $(a_1, \ldots, a_k) \in \mathbb{R}^k \setminus (0, \ldots, 0)$ and $b \in \mathbb{R}$) such that $\mathcal{S} \subset \mathrm{clos}_{\mathrm{Zar}}(\mathcal{S}) \subset H$.

We prove below that $\mathrm{clos}_{\mathrm{Zar}}(\mathcal{S}) \cap \mathbb{R}^k$ is an affine subspace which implies that $\mathrm{clos}_{\mathrm{Zar}}(\mathcal{S})$ is an affine subspace.

From Lemma 3.4, if $\dim(\mathcal{S}) = 0$ then $\mathcal{S}$ is a single point; thus the conclusion follows immediately.

We suppose now that $\dim(\mathcal{S}) > 0$; hence $\mathcal{S}$ is not empty and contains infinitely many points. Consider $y_0 \in \mathcal{S}$. Given $y \in \mathbb{R}^k \setminus \{y_0\}$, we denote by $L_{y_0,y} \subset \mathbb{R}^k$ the real line containing y and y_0 and by $H_{y_0,y} \subset \mathbb{R}^k$ the real affine hyperplane which is orthogonal to $L_{y_0,y}$ and which contains y_0.

Since $\mathcal{S}$ is convex, for all $y \in \mathcal{S} \setminus \{y_0\}$, $\mathcal{S} \cap L_{y,y_0} \neq \emptyset$. We consider the set $\mathcal{U}_{y_0} = \bigcap_{y \in \mathcal{S} \setminus \{y_0\}} H_{y_0,y}$; note that $\mathcal{U}_{y_0}$ is an affine subspace since it is the intersection of affine subspaces. We claim that the orthogonal of $\mathcal{U}_{y_0}$ is $\mathrm{clos}_{\mathrm{Zar}}(\mathcal{S}) \cap \mathbb{R}^k$.

We first prove that $\mathcal{S}$ is contained in the orthogonal of $\mathcal{U}_{y_0}$ which implies that $\mathrm{clos}_{\mathrm{Zar}}(\mathcal{S}) \cap \mathbb{R}^k$ is contained in the orthogonal of $\mathcal{U}_{y_0}$. By definition of $\mathcal{U}_{y_0}$, for all $u \in \mathcal{U}_{y_0}$ and all $y \in \mathcal{S} \setminus \{y_0\}$, the inner product of $\overrightarrow{y_0 u}$ and $\overrightarrow{y_0, y}$ is zero. We prove now that the orthogonal of $\mathcal{U}_{y_0}$ is contained in $\mathrm{clos}_{\mathrm{Zar}}(\mathcal{S}) \cap \mathbb{R}^k$. By definition, the orthogonal of $\mathcal{U}_{y_0}$ is the set of lines L_{y,y_0} for $y \in \mathcal{S} \setminus \{y_0\}$. Thus, it is sufficient to prove that for all $y \in \mathcal{S} \setminus \{y_0\}$, L_{y,y_0} is contained in $\mathrm{clos}_{\mathrm{Zar}}(\mathcal{S}) \cap \mathbb{R}^k$. For all $y \in \mathcal{S} \setminus \{y_0\}$, $\mathcal{S} \cap L_{y,y_0} \neq \emptyset$ because $\mathcal{S}$ is convex. Moreover, $\mathrm{clos}_{\mathrm{Zar}}(\mathcal{S} \cap L_{y,y_0}) \cap \mathbb{R}^k$ is L_{y,y_0}. Since $\mathcal{S} \cap L_{y,y_0} \subset \mathcal{S}$, L_{y,y_0} is contained in $\mathrm{clos}_{\mathrm{Zar}}(\mathcal{S}) \cap \mathbb{R}^k$. Our assertion follows. □

Suppose that $\dim(\mathcal{S}) = k$. Then, by Lemma 3.3, $\mathcal{S} \cap \mathbb{Q}^k$ is not empty and a rational point is outputted at Step (2) by Corollary 2.6. Suppose now that $\mathcal{S}$ is empty. Then, an empty list is returned at Step (4). We suppose now that $\mathcal{S}$ is not empty and that no rational point is outputted at Step (6). Hence, we enter at Step (7).

Remark that the formula Θ (Step (7a)) defines the semi-algebraic set $\mathcal{A} \subset \mathbb{R}^k \times \mathbb{R}$ such that $(a_1, \ldots, a_k, b) \in \mathcal{A}$ if and only if $(a_1, \ldots, a_k) \neq (0, \ldots, 0)$ and

$$\forall (y_1, \ldots, y_k) \in \mathbb{R}^k \quad (y_1, \ldots, y_k) \in \mathcal{S} \Longrightarrow a_1 y_1 + \cdots + a_k y_k = b.$$

Thus, the quantifier-free formula $\bigvee_{i=1}^{I} \Psi_i$ (Step (7b)) defines $\mathcal{A}$. Note that by Lemma 3.6, $\mathcal{A}$ is not empty. Hence, the loop at Step (7c) ends by finding a rational parametrization $\mathcal{G} = (G, G_0, G_1, \ldots, G_k, G_{k+1})$ (computed at Step (7(c)i)) which encodes some points in $\mathcal{A}$.

From the specification of SemiAlgebraicSolve, G is irreducible over $\mathbb{Q}$. Let $a = (a_1, \ldots, a_k) \in \mathbb{R}^k$ and $b \in \mathbb{R}$ such that $(a, b) \in \mathcal{A} \cap Z(\mathcal{G})$. Then, there exists a real root ϑ of G such that

$$G_0(\vartheta) \begin{pmatrix} a \\ b \end{pmatrix} = \sum_{i=1}^{\deg(G)-1} \vartheta^i \begin{pmatrix} \mathbf{a}_i \\ \mathbf{b}_i \end{pmatrix} \tag{4}$$

where the couples $(\mathbf{a}_i, \mathbf{b}_i) \in \mathbb{Z}^k \times \mathbb{Z}$ are those returned by GenerateVectors (Step (7d)). Since $\gcd(G_0, G) = 1$, $G_0(\vartheta) \neq 0$. Moreover, $(a, b) \in \mathcal{A}$ implies $a \neq (0, \ldots, 0)$. Note also that $(a, b) \in \mathcal{A}$ implies that for all $\lambda \in \mathbb{R}^\star$, $(\lambda a, \lambda b) \in \mathcal{A}$ since for all $(y_1, \ldots, y_k) \in \mathcal{S}$ and $\lambda \in \mathbb{R}^\star$

$$a_1 y_1 + \cdots + a_k y_k = b \Longleftrightarrow \lambda(a_1 y_1 + \cdots + a_k y_k) = \lambda b$$

This proves that

$$(a^\star, b^\star) = (G_0(\vartheta) a, G_0(\vartheta) b) \in \mathcal{A} \text{ and } (a_1^\star, \ldots, a_k^\star) \neq (0, \ldots, 0).$$

Thus, there exists i such that $\mathbf{a}_i \neq 0$, which implies that Step (7e) never fails. To end the proof of correctness, we distinguish the case where $\mathcal{S} \cap \mathbb{Q}^k$ is empty or not.

The non-empty case. We suppose first that $\mathcal{S} \cap \mathbb{Q}^k$ is non-empty; let $(y_1, \ldots, y_k) \in \mathcal{S} \cap \mathbb{Q}^k$. Using (4), the linear relation $a_1^\star y_1 + \cdots + a_k^\star y_k = b^\star$ implies the algebraic relation of degree $\deg(G) - 1$:

$$\sum_{i=0}^{\deg(G)-1} \vartheta^i \left(\sum_{j=1}^{k} \mathbf{a}_{i,j} y_j - \mathbf{b}_i\right) = 0, \tag{5}$$

where $\mathbf{a}_{i,j}$ is the j-th coordinate of $\mathbf{a}_i$. Since G is irreducible, it is the minimal polynomial of ϑ; hence ϑ is an algebraic number of degree $\deg(G)$. Thus, (5) is equivalent to

$$\forall 0 \leq i \leq \deg(G) - 1, \quad \sum_{j=1}^{k} \mathbf{a}_{i,j} y_j = \mathbf{b}_i.$$

We previously proved that there exists i such that $\mathbf{a}_i \neq 0$. We let $a = (a_1, \ldots, a_k) \in \mathbb{Z}^k \setminus (0, \ldots, 0)$ and $b \in \mathbb{Z}$ be respectively the vector with integer coordinates and the integer chosen in C (Step (7e)). We have just proved that $\mathcal{S}\cap\mathbb{Q}^k$ is contained in the intersection of $\mathcal{S}$ and of the affine hyperplane H defined by $a_1Y_1+\cdots+a_kY_k=b$. Note also that $\mathcal{S}\cap H$ is convex since $\mathcal{S}$ is convex and H is an affine hyperplane.

Consider the projection $\pi_r:(y_1,\dots,y_k)\in\mathbb{R}^k\to(y_1,\dots,y_{r-1},y_{r+1},\dots,y_k)\in\mathbb{R}^{k-1}$ for the integer r computed at Step (7f). It is clear that the formula Φ' computed at Step (7h) defines the semi-algebraic set $\pi_r(\mathcal{S}\cap H)\subset\mathbb{R}^{k-1}$. Since $\mathcal{S}\cap H$ is convex, $\pi_r(\mathcal{S}\cap H)$ is convex. Thus, the call to FindRationalPoints (Step (7i)) with inputs Φ' and $[Y_1,\dots,Y_{r-1},Y_{r+1},\dots,Y_k]$ is valid. From the induction assumption, it returns a rational point in $\pi_r(\mathcal{S}\cap H)$ if and only if $\pi_r(\mathcal{S}\cap H)$ has a non-empty intersection with $\mathbb{Q}^{k-1}$.

Since $\mathcal{S}\cap\mathbb{Q}^k$ (which is supposed to be non-empty) is contained in $\mathcal{S}\cap H$, $\pi_r(\mathcal{S}\cap H)$ contains rational points. Thus, the list L (Step (7i)) contains a rational point $\mathbf{q}_{k-1}=(q_1,\dots,q_{r-1},q_{r+1},\dots,q_k)\in\pi_r(\mathcal{S}\cap H)$. This implies that $\pi_r^{-1}(\mathbf{q}_{k-1})\cap H$ has a non-empty intersection with $\mathcal{S}\cap H$. Remark that $\pi_r^{-1}(\mathbf{q}_{k-1})\cap H$ is the rational point $\mathbf{q}=(q_1,\dots,q_{r-1},q_r,q_{r+1},\dots,q_k)$ where q_r is computed at Step (7(j)ii). It belongs to $\mathcal{S}$ since $\pi_r^{-1}(\mathbf{q}_{k-1})\cap H$ and $\mathcal{S}\cap H$ have a non-empty intersection. Thus, $\Phi(q_1,\dots,q_{r-1},q_r,q_{r+1},\dots,q_k)$ is true and $\mathbf{q}$ is returned by FindRationalPoints.

The empty case. Suppose now that $\mathcal{S}\cap\mathbb{Q}^k$ is empty. As above H denotes the affine hyperplane defined by $a_1Y_1+\cdots+a_kY_k=b$ where $(a_1,\dots,a_k)\in\mathbb{Z}^k$ and $b\in\mathbb{Z}$ are chosen at Step (7e). Using the above argumentation, $\pi_r(\mathcal{S}\cap H)$ is convex and the formula Φ' (Step (7h)) defines $\pi_r(\mathcal{S}\cap H)$. Thus, the call to FindRationalPoints (Step (7i)) with inputs Φ' and $[Y_1,\dots,Y_{r-1},Y_{r+1},\dots,Y_k]$ is valid. Suppose that $\pi_r(\mathcal{S}\cap H)$ does not contain rational points. Then, by the induction assumption, L is empty and the empty list is returned (Step (7j)) which is the expected output since we have supposed $\mathcal{S}\cap\mathbb{Q}^k=\emptyset$. Else, L contains a rational point $(q_1,\dots,q_{r-1},q_{r+1},\dots,q_k)$. Consider the rational point $(q_1,\dots,q_{r-1},q_r,q_{r+1},\dots,q_k)$ (where q_r is computed at Step (7(j)ii)). It can not belong to $\mathcal{S}$ since we have supposed $\mathcal{S}\cap\mathbb{Q}^k$ is empty. Consequently, $\Phi(q_1,\dots,q_{r-1},q_r,q_{r+1},\dots,q_k)$ is false and the empty list is returned.

4 Complexity

We analyze now the bit complexity of FindRationalPoints.

Proposition 4.1 *Consider a set of polynomials $\mathcal{P}=\{h_1,\dots,h_s\}\subset\mathbb{Z}[Y_1,\dots,Y_k]$, and a quantifier-free $\mathcal{P}$-formula $\Phi(Y_1,\dots,Y_k)$ and let D be an integer such that* $\deg(h_i)\le D$ *for $1\le i\le s$ and σ the maximum bit length of the coefficients of the h_i's. Then,* FindRationalPoints$(\Phi,[Y_1,\dots,Y_k])$ *requires $\sigma^{\mathrm{O}(1)}(sD)^{\mathrm{O}(k^3)}$ bit operations. Moreover, if it outputs a rational point, its coordinates have bit length dominated by $\sigma D^{\mathrm{O}(k^3)}$.*

Remark 4.2 *Let $\mathcal{S}\subset\mathbb{R}^k$ be a convex set defined by*

$$\mathcal{S}=\{Y\in\mathbb{R}^k:\mathbb{R}^k(Q_1X^{[1]}\in\mathbb{R}^{n_1})\cdots(Q_\omega X^{[\omega]}\in\mathbb{R}^{n_\omega})\ P(Y,X^{[1]},\dots,X^{[\omega]})\}$$

with quantifiers $Q_i\in\{\exists,\forall\}$, where $X^{[i]}$ is a set of n_i variables, P is a Boolean function of s atomic predicates

$$g(Y,X^{[1]},\dots,X^{[\omega]})\,\Delta_i\,0$$

where $\Delta_i \in \{>, <, =\}$ (for $i = 1, \dots, s$) and the g_i's are polynomials of degree D with integer coefficients of binary size at most σ. Denote by Θ the quantified formula defining $\mathcal{S}$. By Theorem 2.7, QuantifierElimination(Θ) *requires $\sigma s^{(k+1)\Pi_{i=1}^{\omega}(n_i+1)} D^{(k+1)\Pi_{i=1}^{\omega}\mathrm{O}(n_i)}$ bit operations.*

It outputs a list of conjunctions $\Phi_1, \dots, \Phi_I$ with $I \leq s^{(k+1)\Pi_{i=1}^{\omega}(n_i+1)} D^{(k+1)\Pi_{i=1}^{\omega}\mathrm{O}(n_i)}$, and for $1 \leq i \leq I$, Φ_i is a conjunction of $J_i \leq s^{\Pi_{i=1}^{\omega}(n_i+1)} D^{\Pi_{i=1}^{\omega}\mathrm{O}(n_i)}$ atomic predicates $h \,\Delta\, 0$ with $h \in \mathbb{Z}[Y_1, \dots, Y_k]$, $\Delta \in \{=, >\}$ and $\deg(h) \leq D^{\Pi_{i=1}^{\omega}\mathrm{O}(n_i)}$ and the bit length of the coefficients of the polynomials h_{ij} is dominated by $\sigma D^{(k+1)\Pi_{i=1}^{\omega}\mathrm{O}(n_i)}$. Thus, the cost of running FindRationalPoints *on all the Φ_i's requires $\sigma^{\mathrm{O}(1)}(sD)^{\mathrm{O}(k^3\Pi_{i=1}^{\omega}n_i)}$ bit operations. In case of non-emptiness of $\mathcal{S} \cap \mathbb{Q}^k$, it returns an element of $\mathcal{S} \cap \mathbb{Q}^k$ whose coordinates have bit length dominated by $\sigma D^{\mathrm{O}(k^3\Pi_{i=1}^{\omega}n_i)}$. This ends to prove Corollary 1.2.*

We start with a lemma.

Lemma 4.3 *Steps (1-6) of* FindRationalPoints(Φ) *perform within $\sigma^{\mathrm{O}(1)} s^{k+1} D^{\mathrm{O}(k)}$ bit operations. If a rational point is returned at Step (6) or Step (2), its coordinates have bit length dominated by $\sigma D^{\mathrm{O}(k)}$.*

Proof. The result is a direct consequence of the results stated at Section 2.

1. From Corollary 2.6, Step (1) is performed within $\sigma s^{k+1} D^{\mathrm{O}(k)}$ bit operations and if a rational point is outputted at Step (2), its coordinates have bit length dominated by $\sigma D^{\mathrm{O}(k)}$.

2. From Proposition 2.1, Steps (3) and (4) are performed within $\sigma^{\mathrm{O}(1)} s^{k+1} D^{\mathrm{O}(k)}$ bit operations.

3. From Proposition 2.3, Step (5) requires $\sigma^{\mathrm{O}(1)} D^{\mathrm{O}(k)}$ bit operations. Moreover, if a rational point is outputted at Step (6), its coordinates have bit length dominated by $\sigma D^{\mathrm{O}(k)}$.

□

We prove now the following result.

Lemma 4.4 *1. Steps (7a-7h) require $\sigma^{\mathrm{O}(1)}(sD)^{\mathrm{O}(k^2)}$ bit operations. The number of polynomials in Φ' is s; their degrees are dominated by D and the bit length of their coefficients is dominated by $\sigma D^{\mathrm{O}(k^2)}$.*

2. If a rational point with coordinates of bit length dominated by ℓ is returned at Steps (7i-7j), the rational number computed at Step (7(j)ii) has bit length dominated by $\ell + \sigma D^{\mathrm{O}(k^2)}$.

Proof. From Theorem 2.7, Steps (7a-7b) are performed within $\sigma s^{\mathrm{O}(k^2)} D^{\mathrm{O}(k^2)}$ bit operations. The obtained quantifier-free formula is a disjunction of $(sD)^{\mathrm{O}(k^2)}$ conjunctions. Thus the loop (Step (7c)) makes at most $(sD)^{\mathrm{O}(k^2)}$ calls to SemiAlgebraicSolve. Each conjunctions involves $(sD)^{\mathrm{O}(k)}$ polynomials of degree $D^{\mathrm{O}(k)}$ in $\mathbb{Z}[A_1, \dots, A_k, B]$ with integers of bit length dominated by $\sigma D^{\mathrm{O}(k^2)}$.

Thus, from Proposition 2.1, Step (7(c)i) is performed within $\sigma^{\mathrm{O}(1)}(sD)^{\mathrm{O}(k^2)}$ bit operations and outputs a rational parametrization of degree $D^{\mathrm{O}(k^2)}$ with integer coefficients of bit length dominated by $\sigma D^{\mathrm{O}(k^2)}$. Thus, the integers in the list computed at Step (7d) have bit length dominated by $\sigma D^{\mathrm{O}(k^2)}$. This implies that the polynomial obtained from Steps (7e-7g) has rational coefficients of bit length dominated by $\sigma D^{\mathrm{O}(k^2)}$. Assertion (2) follows immediately.

The bit complexity of these steps is obviously negligible compared to the cost of Step (7(c)i). The substitution phase (Step 7h) has a cost which is still dominated by the cost of Step (7(c)i). As announced, the obtained formula Φ' contains s $(k-1)$-variate polynomials of degree D with integer coefficients of bit length dominated by $\sigma D^{\mathrm{O}(k^2)}$. $\square$

We prove now Proposition 4.1 by induction on k. The initialization of the induction is immediate from Lemmata 3.5 and 4.3.

Suppose that $k > 1$. Suppose that the execution of FindRationalPoints(Φ) stops at Steps (2), or (4) or (6). From Lemma 4.3, we are done. Suppose now that we enter in Step (7).

By Lemma 4.4(1), the formula Φ' computed at Step (7h) contains s $(k-1)$-variate polynomials of degree D and coefficients of bit length dominated by $\sigma D^{\mathrm{O}(k^2)}$ and is obtained within $\sigma^{\mathrm{O}(1)}(sD)^{\mathrm{O}(k^2)}$ bit operations. The induction assumption implies that

- Step (7i) requires $\sigma^{\mathrm{O}(1)}(sD)^{\mathrm{O}(k^3)}$ bit operations,
- If a rational point is contained in L (Step (7j)), its coordinates have bit length dominated by $\sigma D^{\mathrm{O}(k^3)}$.

Hence, by Lemma 4.4(2), the rational number computed at Step (7(j)ii) has bit length dominated by $\sigma D^{\mathrm{O}(k^3)}$. Moreover, the cost of Steps (7(j)ii-7(j)iii) is negligible compared to the cost of previous steps.

5 Rational sums of squares

Consider a polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$ of degree $2d$ whose coefficients have bit length bounded by τ. If we choose v as the vector of all monomials in $\mathbb{Z}[x_1, \ldots, x_n]$ of degree less than or equal to d, then we consider the set of real symmetric matrices $M = M^T$ of dimension $D = \binom{n+d}{n}$ for which $f = \mathrm{v}^T \cdot M \cdot \mathrm{v}$. By Gaussian elimination, it follows that there exists an integer $k \leq \frac{1}{2}D(D+1) - \binom{n+2d}{n}$ such that

$$M = \{M_0 + Y_1 M_1 + \ldots + Y_k M_k,\ Y_1, \ldots, Y_k \in \mathbb{R}\} \tag{6}$$

for some rational symmetric matrices $M_0, \ldots, M_k$. The polynomial f can be written as a sum of squares of polynomials if and only if the matrix M can be completed as a symmetric positive semidefinte matrix (see Laurent (2001)). Let $Y = (Y_1, \ldots, Y_k)$, we define

$$\mathcal{S} = \{Y \in \mathbb{R}^k \mid M(Y) \succeq 0,\ M(Y) = M(Y)^T,\ f = \mathrm{v}^T \cdot M(Y) \cdot \mathrm{v}\}. \tag{7}$$

It is clear that $\mathcal{S} \subseteq \mathbb{R}^k$ is a convex set defined by setting all polynomials in

$$\Phi(Y_1, \ldots, Y_k) = \{(-1)^{(i+D)} m_i,\ i = 0, \ldots, D-1\} \tag{8}$$

to be nonnegative, where the m_i's are the coefficients of the characteristic polynomial of $M(Y)$. The cardinality s of Φ is bounded by D and Φ contains polynomials of degree bounded by D whose coefficients have bit length bounded by

τD (see Powers and Wörmann (1998)). Hence the semi-algebraic set defined by (7) is

$$\mathcal{S} = \{(Y_1, \ldots, Y_k) \in \mathbb{R}^k \mid (-1)^{(i+D)} m_i \geq 0,\ 0 \leq i \leq D-1\}. \tag{9}$$

The result below is obtained by applying Theorem 1.1 to the semi-algebraic set defined above.

Corollary 5.1 *Let $f \in \mathbb{Z}[x_1, \ldots, x_n]$ of degree $2d$ with integers of bit length bounded by τ. By running the algorithm* FindRationalPoints *for the semi-algebraic set defined in (7), one can decide whether f is a sum of squares in $\mathbb{Q}[x_1, \ldots, x_n]$ within $\tau^{\mathrm{O}(1)} D^{\mathrm{O}(k^3)}$ bit operations. Suppose $f = \sum f_i^2, f_i \in \mathbb{Q}[x_1, \ldots, x_n]$, then the bit lengths of rational coefficients of the f_i's are bounded by $\tau D^{\mathrm{O}(k^3)}$.*

Remark 5.2 *Applying Proposition 1.3 by Khachiyan and Porkolab to the semi-algebraic set defined in (7), one can decide whether f is a sum of squares in $\mathbb{Z}[x_1, \ldots, x_n]$ within $\tau^{\mathrm{O}(1)} D^{\mathrm{O}(k^4)}$ operations. Suppose that $f = \sum f_i^2, f_i \in \mathbb{Z}[x_1, \ldots, x_n]$, then the bit lengths of integer coefficients of f_i are bounded by $\tau D^{\mathrm{O}(k^4)}$.*

Porkolab and Khachiyan showed that the non-emptiness of the convex set defined in (7) over the reals can be determined in $\mathrm{O}(kD^4) + D^{\mathrm{O}(\min\{k, D^2\})}$ arithmetic operations over $\ell D^{\mathrm{O}(\min\{k, D^2\})}$-bit numbers, where ℓ is the maximal bit length of the matrices M_i (see Porkolab and Khachiyan (1997)). Suppose $\mathcal{S} \neq \emptyset$, i.e., $f \in \mathbb{Q}[x_1, \ldots, x_n]$ is a sum of m squares in $K[x_1, \ldots, x_n]$ where K is an algebraic extension of $\mathbb{Q}$. If K is a totally real number field, then f is also a sum of squares in $\mathbb{Q}[x_1, \ldots, x_n]$, i.e, $\mathcal{S} \bigcap \mathbb{Q}^n \neq \emptyset$ (see Hillar (2009); Kaltofen (2009)). The following lemma and proof can be deduced from arguments given in Kaltofen (2009).

Lemma 5.3 *Suppose $\mathcal{G} = (G, G_0, G_1, \ldots, G_k)$ is a rational parametrization for the semi-algebraic set $\mathcal{S}$ defined in (7) computed by* SemiAlgebraicSolve. *Suppose ϑ is a real root of G such that*

$$Y(\vartheta) = \frac{1}{q}(G_1(\vartheta), G_2(\vartheta), \ldots, G_k(\vartheta)) \in \mathcal{S}, \tag{10}$$

Then for any real root ϑ_i of G, we have

$$Y(\vartheta_i) = \frac{1}{q}(G_1(\vartheta_i), G_2(\vartheta_i), \ldots, G_k(\vartheta_i)) \in \mathcal{S}. \tag{11}$$

Moreover, if the polynomial G has only real roots, then the point defined by $\frac{1}{\deg G} \sum_{i=1}^{\deg G} Y(\vartheta_i)$ is a rational point in $\mathcal{S}$.

Proof. Since $Y(\vartheta) \in \mathcal{S}$, the matrix $M(Y(\vartheta))$ is positive semidefinite. We can perform the Gaussian elimination over $\mathbb{Q}(\vartheta)$ to obtain the decomposition $M(Y(\vartheta)) = A(\vartheta)^T A(\vartheta)$. It is clear that for any real root ϑ_i of G, $M(Y(\vartheta_i)) = A(\vartheta_i)^T A(\vartheta_i)$ is also positive semi-definite, i.e., $Y(\vartheta_i) \in \mathcal{S}$. Moreover, if G has only real roots ϑ_i, then $\sum_{\vartheta_i, G(\vartheta_i)=0} G_j(\vartheta_i) \in \mathbb{Q}$. It follows that the point defined by $\frac{1}{\deg G} \sum_{i=1}^{\deg G} Y(\vartheta_i)$ is a rational point in $\mathcal{S}$.

□

The above discussion leads to the following result.

Theorem 5.4 *Suppose $f \in \mathbb{Z}[x_1, \ldots, x_n]$. There exists a function* RationalTotalRealSolve *which either determines that f can not be written as sum of squares over the reals or returns a sum of squares representation of f over $\mathbb{Q}[x_1, \ldots, x_n]$ if and only if the polynomial G outputted from the function* SemiAlgebraicSolve *has only real solutions. The coordinates of the rational coefficients of polynomials f_i in $f = \sum_i f_i^2$ have bit length dominated by $\tau D^{O(k)}$ and the bit complexity of* RationalTotalRealSolve *is $\tau^{O(1)} D^{O(k)}$.*

References

Basu, S., Pollack, R., Roy, M.-F., 1996. On the combinatorial and algebraic complexity of quantifier elimination. J. ACM 43 (6), 1002–1045.

Basu, S., Pollack, R., Roy, M.-F., 2006. Algorithms in real algebraic geometry, 2nd Edition. Vol. 10 of Algorithms and Computation in Mathematics. Springer-Verlag.

Bochnak, J., Coste, M., Roy, M.-F., 1998. Real Algebraic Geometry. Springer-Verlag.

Choi, M., Lam, T., Reznick, B., 1995. Sums of squares of real polynomials. Symp. in Pure Math. 58 (2), 103–126.

Heinz, S., 2005. Complexity of integer quasiconvex polynomial optimization. J. Complex. 21 (4), 543–556.

Hillar, C., 2009. Sums of polynomial squares over totally real fields are rational sums of squares. Proc. American Math. Society 137, 921–930.

Kaltofen, E., Li, B., Yang, Z., Zhi, L., 2008. Exact certification of global optimality of approximate factorizations via rationalizing sums-of-squares with floating point scalars. In: Proc. ISSAC08. pp. 155–163.

Kaltofen, E., Li, B., Yang, Z., Zhi, L., jan 2009. Exact certification in global polynomial optimization via sums-of-squares of rational functions with rational coefficients. Manuscript, 20 pages.

Kaltofen, E. L., 2009. Private communication, February 24, 2009.

Khachiyan, L., Porkolab, L., 1997. Computing integral points in convex semialgebraic sets. Foundations of Computer Science, Annual IEEE Symposium on 0, 162–171.

Khachiyan, L., Porkolab, L., 2000. Integer optimization on convex semialgebraic sets. Discrete and Computational Geometry 23 (2), 207–224.

Laurent, M., 2001. Polynomial instances of the positive semidefinite and euclidean distance matrix completion problems. SIAM J. Matrix Anal. Appl. 22 (3), 874–894.

Lenstra, A. K., H. W. Lenstra, H. W., Lovàsz, L., 1982. Factoring polynomials with rational coefficients. Math. Ann. 261, 515–534.

Lenstra, H. W., J., 1983. Integer programming with a fixed number of variables. Mathematics of Operations Research 8 (4), 538–548.
URL http://www.jstor.org/stable/3689168

Mignotte, M., 1982. Some useful bounds. In: Buchberger, B., Collins, G. E., Loos, R. (Eds.), Computer Algebra, Symbolic and Algebraic Computation. Supplementum to Computing. Springer Verlag, pp. 259–263.

Peyrl, H., Parrilo, P. A., 2007. A Macaulay 2 package for computing sum of squares decompositions of polynomials with rational coefficients. In: Proc. SNC'07. pp. 207–208.

Peyrl, H., Parrilo, P. A., 2008. Computing sum of squares decompositions with rational coefficients. Theoretical Computer Science 409, 269–281.

Porkolab, L., Khachiyan, L., 1997. On the complexity of semidefinite programs. J. of Global Optimization 10 (4), 351–365.

Powers, V., Wörmann, T., 1998. An algorithm for sums of squares of real polynomials. Journal of Pure and Applied Algebra 6 (1), 99–104.

Schönhage, A., 1984. Factorization of univariate integer polynomials by diophantine aproximation and an improved basis reduction algorithm. In: ICALP. pp. 436–447.

van Hoeij, M., Novocin, A., 2007. Complexity results for factoring univariate polynomials over the rationals. Preprint, URL: http://www.math.fsu.edu/ hoeij/papers/2007/paper6.pdf.

Centre de recherche INRIA Paris – Rocquencourt
Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Grenoble – Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier
Centre de recherche INRIA Lille – Nord Europe : Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq
Centre de recherche INRIA Nancy – Grand Est : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Saclay – Île-de-France : Parc Orsay Université - ZAC des Vignes : 4, rue Jacques Monod - 91893 Orsay Cedex
Centre de recherche INRIA Sophia Antipolis – Méditerranée : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399